

ELLIPTIC CURVES AND BIQUADRATES

JULIÁN AGUIRRE AND JUAN CARLOS PERAL

ABSTRACT. Given two integers m and n consider $N = m^4 + n^4$ and the elliptic curve

$$y^2 = x^3 - Nx$$

The rank of this family over $\mathbb{Q}(m, n)$ is at least 2.

Euler constructed a parametric family of integers N expressible in two different ways as a sum of two biquadrates. We prove that for those N the corresponding family of elliptic curves has rank at least 4 over $\mathbb{Q}(u)$. This is an improvement on previous results of Izadi, Khoshnam and Nabardi.

1. SUMS OF TWO BIQUADRATES AND ELLIPTIC CURVES

1.1. Elliptic curves and sums of biquadrates. General case. For integers m and n consider the elliptic curves given by

$$(1) \quad y^2 = x^3 - (m^4 + n^4)x.$$

The torsion groups for elliptic curves of the form $y^2 = x^3 + Dx$ are, $\mathbb{Z}/4\mathbb{Z}$ for $D = 4$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for $D = -h^2$ and $\mathbb{Z}/2\mathbb{Z}$ in the rest of the cases (see [S], Proposition 6.1, p. 311). This together with the fact that $h^2 = m^4 + n^4$ has no solution (see [HW], Theorem 266) implies that the torsion group for the curves (1) is always $\mathbb{Z}/2\mathbb{Z}$. We have proved the following

Theorem 1. *The family (1) has rank at least 2 over $\mathbb{Q}(m, n)$.*

To estimate the rank we study the existence of generic points on these curves and their associates. The identity

$$(-1)(n)^4 + \frac{-(m^4 + n^4)}{-1} (1)^4 = m^4$$

reveals that for $d = -1$ the homogenous space $(U)^4d + (-N/d)V^4 = H^2$ has the solution $(U, V, H) = (n, 1, m^2)$, and this implies that the point $P_1 = (-n^2, m^2n)$ is on the curve.

For the associated curve $y^2 = x^3 + 4(m^4 + n^4)x$ we have the identity

$$(2)(m+n)^4 + \frac{4(m^4 + n^4)}{2} = (2(m^2 + n^2 + mn))^2,$$

so that for $d = 2$ the homogenous space $(U)^4d + (4N/d)V^4 = H^2$ has the solution $(U, V, H) = (m+n, 1, 2(m^2 + n^2 + mn))$.

Consequently the point $Q_1 = (2(m+n)^2, 4(m+n)(m^2 + mn + n^2))$ is on the curve. We transfer Q_1 to the main curve, and we have two points on that curve given by:

$$P_1(m, n) = \{-n^2, m^2n\},$$

$$P_2(m, n) = \left\{ \frac{(m^2 + mn + n^2)^2}{(m+n)^2}, \frac{mn(m^2 + mn + n^2)(2m^2 + 3mn + 2n^2)}{(m+n)^3} \right\}.$$

2010 *Mathematics Subject Classification.* 14H52.

J. Aguirre supported by grant IT-305-07 of the Basque Government. J.C. Peral supported by the UPV/EHU grant EHU 10/05.

In order to prove that the family (1) has rank at least 2 over $\mathbb{Q}(m, n)$, it suffices to find a specialization $(m, n) = (m_0, n_0)$ such that the points $P_1(m_0, n_0)$, and $P_2(m_0, n_0)$ are independent points on the specialized curve over \mathbb{Q} , due to the fact that the specialization is a homomorphism (see [S].) For $(m_0, n_0) = (2, 1)$ the curve is $y^2 = x^3 - 17x$ and the points are

$$P_1(2, 1) = \{-1, 4\},$$

$$P_2(2, 1) = \left\{\frac{49}{9}, \frac{224}{27}\right\}.$$

The curve has rank 2 over \mathbb{Q} and the points are independent as can be checked with the program `mwrank` [C]. So the rank of the family (1) is at least 2 over $\mathbb{Q}(m, n)$.

1.2. Examples with bigger rank. We have found, after a short search, many examples of curves with rank 7 over \mathbb{Q} , eight examples of curves with rank 8 over \mathbb{Q} and one example with rank 9. The smaller values of N that we found, in the case of rank 7, are:

$$\begin{aligned} 3534242722 &= 83^4 + 243^4 \\ 3730925026 &= 125^4 + 243^4 \\ 3732157186 &= 155^4 + 237^4 \\ 3840351442 &= 147^4 + 241^4 \\ 9633078002 &= 77^4 + 313^4 \\ 26939353666 &= 77^4 + 405^4 \\ 71486456242 &= 81^4 + 517^4 \end{aligned}$$

The curves with rank 8 correspond to the following values of N :

$$\begin{aligned} 25792915457 &= 326^4 + 347^4 \\ 141262310897 &= 88^4 + 613^4 \\ 436341291697 &= 631^4 + 726^4 \\ 9788096042497 &= 972^4 + 1727^4 \\ 106232596858561 &= 491^4 + 3210^4 \\ 159764080671457 &= 1191^4 + 3544^4 \\ 202891791817457 &= 1652^4 + 3739^4 \\ 380344532478577 &= 3513^4 + 3886^4 \end{aligned}$$

Finally, for $N = 228746044559762 = 2387^4 + 3743^4$ the curve $y^2 = x^3 - Nx$ has rank 9.

1.3. Euler parametrization. The problem of finding integers expressible in two different ways as sum of two fourth powers has been studied by several authors, see the second volume of the History of Number Theory ([DI], p. 644–648). In particular, Euler constructed a bi-parametric family of solutions of $N = A^4 + B^4 = C^4 + D^4$ given as follows:

$$\begin{aligned} A(u, w) &= u(u^6 + u^4w^2 - 2u^2w^4 + 3uw^5 + w^6), \\ B(u, w) &= w(u^6 - 3u^5w - 2u^4w^2 + u^2w^4 + w^6), \\ C(u, w) &= u(u^6 + u^4w^2 - 2u^2w^4 - 3uw^5 + w^6), \\ D(u, w) &= w(u^6 + 3u^5w - 2u^4w^2 + u^2w^4 + w^6). \end{aligned}$$

In what follows we take $w = 1$. There is no loss of generality with this choice due to the homogeneity. Then

$$\begin{aligned}
 (2) \quad N &= A(u, 1)^4 + B(u, 1)^4 \\
 &= C(u, 1)^4 + D(u, 1)^4 \\
 &= (1 + 6u^2 + u^4)(1 - u^4 + u^8)(1 - 4u^2 + 8u^4 - 4u^6 + u^8) \\
 &\quad \times (1 + 2u^2 + 11u^4 + 2u^6 + u^8).
 \end{aligned}$$

1.4. Elliptic curves and sums of biquadrates. Case of two equal sums.

Now we consider the curves

$$(3) \quad y^2 = x^3 - Nx$$

where N is given by (2). Subsection 1.1 and the fact that N can be expressed in two different ways as sum of two biquadrates suggest that the subfamily (3) has a greater rank than the general family (1), and that this generic rank has to be at least 4.

In [IKN] the authors prove that if N is square free, then the rank of (3) over $\mathbb{Q}(u)$ is at least 3. They also prove, assuming the Parity Conjecture and some other conditions, that the rank is at least 4. We improve their result by proving in the next theorem that the rank is at least 4 over $\mathbb{Q}(u)$ unconditionally.

Theorem 2. *The rank of (3) over $\mathbb{Q}(u)$ is at least 4.*

Proof. We proceed, as in the general case, searching solutions in the homogenous spaces $dU^4 - (N/d)V^4 = H^2$ of the curve, where d is a divisor of N .

There is one solution for $(U, V) = (1, 1)$ and the divisor $d = (1 - u^4 + u^8)(1 + 2u^2 + 11u^4 + 2u^6 + u^8)$, and another one for $(U, V) = (A(u), 1) = (u(1 + 3u - 2u^2 + u^4 + u^6), 1)$ for the divisor $d = -1$. These two solutions produce the corresponding two points on the curve given by

$$\begin{aligned}
 P_1(u) &= \{(1 - u^4 + u^8)(1 + 2u^2 + 11u^4 + 2u^6 + u^8), \\
 &\quad u^2(-5 + 4u^2 + u^4 + u^6)(1 - u^4 + u^8)(1 + 2u^2 + 11u^4 + 2u^6 + u^8)\}, \\
 P_2(u) &= \{-u^2(1 + 3u - 2u^2 + u^4 + u^6)^2, \\
 &\quad u(1 + 3u - 2u^2 + u^4 + u^6)(1 + u^2 - 2u^4 - 3u^5 + u^6)^2\}.
 \end{aligned}$$

We perform a similar search in the homogenous spaces of the associated curve $y^2 = x^3 + 4Nx$. In this case we observe the existence of solutions for $(U, V) = (A(u) + B(u), 1) = (1 + u + 4u^2 - 2u^3 - 2u^4 - 2u^5 + u^6 + u^7, 1)$ and $d = 2$, and for $(U, V) = (u, 1)$ and $d = 4(1 + 6u^2 + u^4)(1 + 2u^2 + 11u^4 + 2u^6 + u^8)$.

Again we have the corresponding points on the associated curve given by

$$\begin{aligned}
 Q_1(u) &= \{2(1 + u + 4u^2 - 2u^3 - 2u^4 - 2u^5 + u^6 + u^7)^2, \\
 &\quad 4(1 + u + 4u^2 - 2u^3 - 2u^4 - 2u^5 + u^6 + u^7) \\
 &\quad \times (1 + u + 6u^2 + 5u^3 + 5u^4 - 21u^5 - 5u^6 - 2u^7 + 13u^8 \\
 &\quad + 15u^9 - u^{10} - 7u^{11} + u^{13} + u^{14})\} \\
 Q_2(u) &= \{4u^2(1 - u^4 + u^8)(1 - 4u^2 + 8u^4 - 4u^6 + u^8), \\
 &\quad \times 4u(1 - u^4 + u^8)(1 - 4u^2 + 8u^4 - 4u^6 + u^8) \\
 &\quad \times (1 + 4u^2 + 6u^4 + 3u^6 - 4u^8 + 2u^{10})\}.
 \end{aligned}$$

We transfer points $Q_1(u)$ and $Q_2(u)$ to the original curve and jointly with P_1 and P_2 , we get four points whose x -coordinates are:

$$\begin{aligned} x_1(u) &= (1 - u^4 + u^8)(1 + 2u^2 + 11u^4 + 2u^6 + u^8), \\ x_2(u) &= -u^2(1 + 3u - 2u^2 + u^4 + u^6)^2, \\ x_3(u) &= \frac{(1 + 4u^2 + 6u^4 + 3u^6 - 4u^8 + 2u^{10})^2}{4u^2}, \\ x_4(u) &= (1 + u + 6u^2 + 5u^3 + 5u^4 - 21u^5 - 5u^6 - 2u^7 + 13u^8 \\ &\quad + 15u^9 - u^{10} - 7u^{11} + u^{13} + u^{14})^2 \\ &\quad / (1 + u + 4u^2 - 2u^3 - 2u^4 - 2u^5 + u^6 + u^7)^2. \end{aligned}$$

We finish proving that the rank is at least 4, arguing as before. We choose $u = 2$. The curve is $y^2 = x^3 - 635318657x$ and its rank is 4. The points are

$$\begin{aligned} P_1 &= \{137129, 49914956\}, \\ P_2 &= \{-24964, 549998\}, \\ P_3 &= \left\{ \frac{1766241}{16}, \frac{2285325807}{64} \right\}, \\ P_4 &= \left\{ \frac{365689129}{9801}, \frac{5156125463944}{970299} \right\}. \end{aligned}$$

A calculation with `mwrnk` [C] shows that the four points are independent. This implies, by an specialization argument, that the rank of the family over $\mathbb{Q}(u)$ is at least 4, see [S].

An alternative proof follows by considering directly the steps in the 2-descent argument for curves of the shape $y^2 = x^3 + Ax^2 + Bx$, see [ST]. \square

Remark. Imposing conditions that force the root number to be equal to -1 it is possible to find a subfamily with rank at least 5 over $\mathbb{Q}(u)$ but in this case the result is conditional to the validity of the Parity Conjecture.

Remark. The construction given above suggest that if we had families of integers N with many different representations as sum of two fourth powers, then it would be possible to construct families of elliptic curves, and examples of elliptic curves, having large ranks. Unfortunately, not even a single example with three different representations is known, see [G]. Moreover, a simple heuristic density argument tell us that the possibility to find multiple representations of that form it is very unlikely.

1.5. Examples with bigger rank. In [IKN] the authors quote several examples of rank 8 curves within this family, but all of them reduce to one because the corresponding values of N differ by a fourth power factor. It is the first one in the following list. We have found another value of N , the second one, for which the corresponding curve also has rank 8 over \mathbb{Q} .

$$\begin{aligned} 155974778565937 &= 1623^4 + 3494^4 = 2338^4 + 3351^4 \\ 2701104520630058561 &= 2513^4 + 40540^4 = 11888^4 + 40465^4 \end{aligned}$$

Computations using this family are highly time-consuming because of the size of the coefficients.

Remark. Curves of the form $y^2 = x^3 + Bx$ have j -invariant equal to 1728 and have been studied by many authors, see for example [SH], [F], [N] and [ACP] and the references given there. An example with rank 14 was found by Watkins within the family constructed in [ACP].

Remark. A more detailed version of this note will appear elsewhere.

REFERENCES

- [ACP] Aguirre, J., Castañeda, F., Peral, J.C. *High rank elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z}$* , Mathematics of Computation, **73**, n. 245, pg. 323–331 (2003)
- [C] Cremona J., Algorithms for Modular Elliptic Curves, Cambridge University Press, Cambridge, 1997.
- [F] Fermigier, S. *Construction of high-rank elliptic curves over \mathbb{Q} and $\mathbb{Q}(t)$ with nontrivial 2-torsion*, in Algorithmic Number Theory (Talence 1996) Springer, Berlin.
- [DI] Dickson, L.E. History of the Theory of Numbers, Carnegie Institution, Washington, 1919.
- [HW] Hardy, G.H., Wright, E.M. An introduction to the theory of numbers, Oxford Publications, 1938, (reprinted in 1983)
- [IKN] Izadi, F.A., Khoshnam, F., Nabardi, K. *Sum of two biquadrates and elliptic curves of rank ≥ 4* , preprint, arXiv:1202.5676v2.
- [G] Guy, R.H. Unsolved problems in number theory, Springer-Verlag, New York, 1981.
- [N] Nagao, K., *On the rank of the elliptic curves $y^2 = x^3 - kx$* , Kobe J. Math., **11** (1994), 205–211.
- [S] Silverman, J.H. The arithmetic of elliptic curves, Springer-Verlag, New York, 1986.
- [SH] Shioda, T. *Construction of elliptic curves with high rank via the invariants of the Weyl groups*, J. Math. Soc. Japan, **43** (1991), 673–719.
- [ST] Silverman, J.H., Tate, J. Rational points on elliptic curves, Springer-Verlag, New York, 1992.

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DEL PAÍS VASCO, UPV/EHU, APTDO.
644, 48080 BILBAO, SPAIN
E-mail address, J. Aguirre: julian.aguirre@ehu.es

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DEL PAÍS VASCO, UPV/EHU, APTDO.
644, 48080 BILBAO, SPAIN
E-mail address, J.C. Peral: juancarlos.peral@ehu.es